WE CLAIM

1. A data processing apparatus having a secure domain and a non-secure domain, in the secure domain the data processing apparatus having access to secure data which is not accessible in the non-secure domain, the data processing apparatus comprising:

a device bus;

a device coupled to the device bus and operable to issue a memory access request pertaining to either said secure domain or said non-secure domain; and

a memory coupled to the device bus and operable to store data required by the device, the memory comprising secure memory for storing secure data and non-secure memory for storing non-secure data;

the device being operable to issue onto the device bus the memory access request when access to an item of data in the memory is required, the memory access request issued by the device including a domain signal identifying whether the memory access request pertains to said secure domain or said non-secure domain.

2. A data processing apparatus as claimed in Claim 1, wherein the device is operable in a plurality of modes, including at least one non-secure mode being a mode in the non-secure domain and at least one secure mode being a mode in the secure domain.

3. A data processing apparatus as claimed in Claim 1, wherein the device has a predetermined pin for outputting the domain signal onto the device bus.

4. A data processing apparatus as claimed in Claim 1, wherein in said non-secure domain the device is operable under the control of a non-secure operating system, and in said secure domain the device is operable under the control of a secure operating system.

5. A data processing apparatus as claimed in Claim 1, further comprising partition checking logic coupled to the device bus and operable whenever the memory access request as issued by the device pertains to said non-secure domain to detect if the

memory access request is seeking to access the secure memory, and upon such detection to prevent the access specified by that memory access request.

6. A data processing apparatus as claimed in Claim 5, wherein the partition checking logic is managed by the device when operating in a predetermined secure mode in said secure domain.

7. A data processing apparatus as claimed in Claim 5, wherein the partition checking logic is provided within an arbiter coupled to the device bus to arbitrate between memory access requests issued on the device bus.

8. A data processing apparatus as claimed in Claim 1, wherein the device is a chip incorporating a processor, the chip further comprising a memory management unit operable, when the processor generates the memory access request, to perform one or more predetermined access control functions to control issuance of the memory access request onto the device bus.

9. A data processing apparatus as claimed in Claim 8, wherein the chip further comprises:

further memory coupled to the processor via a system bus, the further memory operable to store data required by the processor, the further memory comprising secure further memory for storing secure data and non-secure further memory for storing non-secure data; and

further partition checking logic coupled to the system bus and operable whenever the memory access request is generated by the processor when operating in a non-secure mode in said non-secure domain to detect if the memory access request is seeking to access either the secure memory or the secure further memory, and upon such detection to prevent the access specified by that memory access request.

10. A method of accessing a memory in a data processing apparatus having a secure domain and a non-secure domain, in the secure domain the data processing apparatus having access to secure data which is not accessible in the non-secure domain,

the data processing apparatus comprising a device bus, a device coupled to the device bus and operable to issue a memory access request pertaining to either said secure domain or said non-secure domain, and a memory coupled to the device bus and operable to store data required by the device, the memory comprising secure memory for storing secure data and non-secure memory for storing non-secure data, the method comprising the steps of:

(i) issuing from the device onto the device bus the memory access request when access to an item of data in the memory is required; and

(ii) including within the memory access request a domain signal identifying whether the memory access request pertains to said secure domain or said non-secure domain.

11. A method as claimed in Claim 10, wherein the device is operable in a plurality of modes, including at least one non-secure mode being a mode in the non-secure domain and at least one secure mode being a mode in the secure domain.

12. A method as claimed in Claim 10, wherein the device has a predetermined pin for outputting the domain signal onto the device bus.

13. A method as claimed in claim 10, wherein in said non-secure domain the device is operable under the control of a non-secure operating system, and in said secure domain the device is operable under the control of a secure operating system.

14. A method as claimed in claim 10, further comprising the steps of:

(iii) whenever the memory access request as issued by the device pertains to said non-secure domain, employing partition checking logic coupled to the device bus to detect if the memory access request is seeking to access the secure memory; and

(iv) upon such detection, preventing the access specified by that memory access request.

15. A method as claimed in Claim 14, wherein the partition checking logic is managed by the device when operating in a predetermined secure mode in said secure domain.

16. A method as claimed in Claim 14, wherein the partition checking logic is provided within an arbiter coupled to the device bus to arbitrate between memory access requests issued on the device bus.

17. A method as claimed claim 10, wherein the device is a chip incorporating a processor, the chip further comprising a memory management unit, when the processor generates the memory access request, the method comprising the step of:

employing the memory management unit to perform one or more predetermined access control functions to control issuance of the memory access request onto the device bus.

18. A method as claimed in Claim 17, wherein the chip further comprises further memory coupled to the processor via a system bus, the further memory operable to store data required by the processor, the further memory comprising secure further memory for storing secure data and non-secure further memory for storing non-secure data, and further partition checking logic coupled to the system bus, the method further comprising the steps of:

whenever the memory access request is generated by the processor when operating in a non-secure mode in said non-secure domain, employing the further partition checking logic to detect if the memory access request is seeking to access either the secure memory or the secure further memory; and

upon such detection, preventing the access specified by that memory access request.

19. A data processing apparatus, comprising:

a device bus;

a device coupled to the device bus and operable in a plurality of modes and either a secure domain or a non-secure domain, including at least one non-secure mode being a mode in the non-secure domain and at least one secure mode being a mode in the secure domain; and

a memory coupled to the device bus and operable to store data required by the device, the memory comprising secure memory for storing secure data and non-secure memory for storing non-secure data;

the device being operable to issue onto the device bus a memory access request when access to an item of data in the memory is required, the memory access request issued by the device including a domain signal identifying whether the device is operating in said at least one secure mode or said at least one non-secure mode.

20. A method of accessing a memory in a data processing apparatus, the data processing apparatus comprising a device bus, a device coupled to the device bus and operable in a plurality of modes and either a secure domain or a non-secure domain, including at least one non-secure mode being a mode in the non-secure domain and at least one secure mode being a mode in the secure domain, and a memory coupled to the device bus and operable to store data required by the device, the memory comprising secure memory for storing secure data and non-secure memory for storing non-secure data, the method comprising the steps of:

(i) issuing from the device onto the device bus a memory access request when access to an item of data in the memory is required; and

(ii) including within the memory access request a domain signal identifying whether the device is operating in said at least one secure mode or said at least one non-secure mode.